

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH
RCHUTCHENS87@GMAIL.COM THAT IS STORED AT
PREMISES CONTROLLED BY GOOGLE LLC

Case No.

1:23-mj-200-LPA
177

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1956	Money Laundering

The application is based on these facts:

See Attached Affidavit of Special Agent Jason Baumgardner

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

On this day, the applicant appeared before me by reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

/s/ Jason Baumgardner

Applicant's signature

Jason Baumgardner, Special Agent, IRS-CI

Printed name and title

Date:

05/05/23



Judge's signature

City and state: Greensboro, North Carolina

United States Magistrate Judge L. Patrick Auld

Printed name and title

Attachment A

Property to Be Searched

This warrant applies to information associated with the account **rchutchens87@gmail.com** that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Attachment B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) – **Google Reference Number 31958844**, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from October 1, 2022 to Present:

- a. All records, files, and other information (including data and the content of electronic communications or contained in “draft” or “trash” Gmail folders) for the Google Services of Drivesync Invite, Gmail, Google Calendar, Google Docs, Google Photos, Google Drive, Google Talk, and Web History associated with the account username;
- b. The contents of all communications including text messages, voicemails, recorded calls, emails, and chat messages associated with the account, including stored or preserved copies of chat logs, emails sent to and from the account, draft communications, the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account

status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- d. All device information associated with the account;
- e. All location history associated with the account;
- f. All search and browsing history associated with the account;
- g. All Google Bookmarks;
- h. All voice and audio activity associated with the account;
- i. Any account trustees or managers associated with the account;
- j. The types of service utilized;
- k. All records or other information stored since October 1, 2022 to the present by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

l. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

m. For all Google accounts that are linked to any of the accounts listed in Attachment A by cookies, creation IP address, recovery email address, or telephone number, provide:

- 1. Names (including subscriber names, usernames, and screen names);
- 2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
- 3. Local and long-distance telephone connection records;
- 4. Records of session times and durations and IP history log;
- 5. Length of service (including start date) and types of service utilized;

6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), MSISDN, International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Station Equipment Identities (“IMEI”));
7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

II Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering), and/or 18 U.S.C. § 1343 (Wire Fraud), and aiding and abetting of these offenses, for each account or identifier listed on Attachment A, in the form of the following:

- (a) Evidence referencing the identity of the individual(s) with access to the email account;
- (b) Records revealing the identity of the person(s) who created or used the email account, including records that help reveal the whereabouts of such person(s);
- (c) Communications amongst any co-conspirators, and between co-conspirators and unwitting individuals, regarding the fraudulent sale of real property;

- (d) Evidence of payments made or received related to the fraudulent sale of real property;
- (e) Evidence of the development or use of fictitious company websites;
- (f) The identity of the persons who communicated with the email account about the fraudulent sale of real property and/or financial transactions related thereto, including records that help reveal their whereabouts; and
- (g) Evidence identifying other email accounts used by the account owner.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
RCHUTCHENS87@GMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE LLC

Case No. 1:23mj177

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Jason Baumgardner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the email account rchutchens87@gmail.com ("SUBJECT EMAIL ACCOUNT").
2. The information associated with the SUBJECT EMAIL ACCOUNT is stored at premises controlled by the following company: Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 ("EMAIL PROVIDER").
3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information to be searched and seized (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. I am a Special Agent with the Internal Revenue Service Criminal Investigation (“IRS-CI”) and have been since 2005. As a Special Agent, I am charged with investigating violations of federal revenue laws and related offenses. I have worked with investigators in federal, state and local law enforcement agencies. I have written affidavits for search and seizure warrants relative to tax and non-tax violations.

5. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, review of documents and records related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information provided in this affidavit is supported by my training, experience, education, and participation in this and other financial investigations.

6. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of 18 U.S.C. § 1956 (Money Laundering) and 18 U.S.C. § 1343 (Wire Fraud) (the “TARGET OFFENSES”) have been committed by RANDALL HUTCHENS (hereinafter HUTCHENS). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(a), and

(c)(1)(a). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offenses being investigated.” 18 U.S.C. § 2711(3)(a)(i).

DEFINITION OF TERMS

8. An “email header” is text at the beginning of an email message. It is generated by the client mail program that first sends it and updated by all the mail servers en route to the destination. Each mail server adds more text, including from/to addresses, subject, content type, time stamp and identification data. You can trace the path of the message from source to destination by reviewing the email header text. Many end user email programs hide this information from the user unless they specifically request to view it.

9. An internet cookie file, or “cookie,” is a file that a website stores on a user’s computer. The website can read the “cookie” and collect information about the computer on which the cookie has been saved. For example, a cookie might be used to track a user’s account on the website, a user’s preferences, or items in the user’s electronic shopping cart.

THE INVESTIGATION

10. Beginning in February 2023, IRS-CI, along with the Cabarrus County Sheriff’s Office (hereinafter CCSO), began investigating HUTCHENS, upon receipt of information that HUTCHENS is advertising real estate for sale on various social media sites and craigslist.org that he does not own nor is he connected to the actual owners in any way. Specifically, on February 27, 2023, A.G. contacted the CCSO to report a fraudulent real estate transaction. A.G. indicated that on December 12, 2022, s/he responded to a Facebook Marketplace listing for a parcel of land for sale at 4875 Yellow Poplar Lane, Concord, Cabarrus County, North Carolina. HUTCHENS placed the ad using his Facebook account with a photo resembling his North Carolina driver’s license photo.

11. A.G. stated that s/he signed a contract with HUTCHENS to purchase the property for \$46,000 and made a \$31,000 down payment with a Wells Fargo cashier's check with the remaining payments of \$250 per month due via Zelle, an electronic payment service. HUTCHENS provided the SUBJECT EMAIL ACCOUNT as the email associated with his Zelle account. In addition, HUTCHENS sent a payment statement to A.G. via email from the SUBJECT EMAIL ACCOUNT. A.G. later discovered from the county clerk's office that the property in question was never owned by HUTCHENS. Both HUTCHENS' posts to the online Facebook Marketplace, as well as the bank transfers from Zelle that he facilitated, were interstate wire signals.

12. On December 27, 2022, an individual known as A.S. sent a text message to HUTCHENS using his phone number 980-255-2219, inquiring about a property HUTCHENS had listed for sale: 6111 Blue Ridge Drive, Concord, North Carolina. HUTCHENS responded that he had thirteen offers on the property already but if A.S. was interested in buying the property, he would sell it to her/him on that same day. During the text message exchanges, HUTCHENS stated that all the activity on the property was making him a little bit crazy because he is a 70-year-old retiree. HUTCHENS explained to A.S. that he had several appointments that day to meet with buyers but if s/he wanted to come in first s/he could buy the property.

13. Later that day on December 27, 2022, A.S. met with HUTCHENS and made a down payment of \$10,000 via cashier's check payable to HUTCHENS and signed a contract to finance the remaining amount payable in \$250 monthly payments. HUTCHENS sent an email to A.S. requesting that payments be made to him via his Zelle account registered to the SUBJECT EMAIL ACCOUNT. On January 23 and February 24, 2023, HUTCHENS emailed A.S. monthly statements reflecting payments and interest for the property located at 6111 Blue Ridge Drive, Concord, Cabarrus County, North Carolina, from the SUBJECT EMAIL ACCOUNT.

14. On March 10, 2023, CCSO detectives spoke with V.K., who is an owner of a real estate investment company. V.K. stated s/he had been paying HUTCHENS for four different properties for which s/he had signed contracts. The properties are: 6111 Blue Ridge Drive and 827 Pitts School Road, in Cabarrus County; and 9233 Old Moore Chapel Road and 6020 Milhaven Lane, in Mecklenburg County. V.K. provided copies of the contracts for each property that s/he and HUTCHENS had signed and were notarized by UPS Store employees. V.K. paid HUTCHENS \$65,000 in total for down payments on these four properties between December 2022 and February 2023.

15. V.K. showed detectives a picture HUTCHENS sent of a Commissioners Deed which was supposed to be the proof of ownership. Only the front page of the deed was shown. According to county land records and property deed searches, HUTCHENS does not own any of the properties listed in the previous paragraph and never has.

16. Cabarrus County property records showed that the property at 6111 Blue Ridge Drive was sold in January 2023 to A.W. but HUTCHENS was not a party to the sale. On March 21, 2023, CCSO detectives spoke with the current property owner of 6111 Blue Ridge Drive. A.W. provided copies of the paperwork where s/he purchased the property and the current deed. A.W. stated s/he does not know HUTCHENS and is not listing the property for sale.

17. A review of HUTCHENS' bank records revealed numerous large, whole dollar cashier's checks being deposited into his bank account from different individuals. The memo line of numerous cashier's checks referenced "6111 Blue Ridge Drive." HUTCHENS deposited additional cashier's checks also noting other addresses in the memo line. A search of property records revealed HUTCHENS did not own the properties referenced in the memo line of these checks.

18. Based on my training and experience, I know that often fraudsters will utilize email to communicate with their potential victims. I also know that in order to facilitate their fraudulent schemes, fraudsters will utilize email communication to provide fictitious documents to victims or co-conspirators, such as fictitious property deeds, sales contracts, payment receipts, loan documents, etc. In order to conduct the scheme, the fraudsters, potential co-conspirators, and victims have to communicate. They often do so through emails, text messages, and instant messenger accounts.

19. There are many reasons why criminal offenders maintain electronic communication evidence for long periods of time. Information such as victims' personal identifying information (PII) has value, as it may be sold, used for other purposes, or reused for the same purpose in future years. Additionally, electronic communication is often stored on third party servers, and may not actually be deleted immediately, even if put into a "deleted items folder" or "trash." The criminal offender may no longer realize that they still possess the evidence, or they may believe that law enforcement could not obtain a search warrant to seize the evidence.

20. In many instances, fraudsters also communicate with individuals not involved in the conspiracy for purposes of using them unwittingly in their scheme. For example, fraudsters will befriend individuals online and convince them to receive money from a source unknown to that person and forward it on to the fraudster. Although the fraudster usually uses a false identity in these email communications, the items being discussed could provide information or evidence that can be used to further identify the identity thief or trace the fraudulent refunds.

21. Based on my training and experience, I also know that fraudsters often use email to communicate about other matters that may provide evidence as to the identity and location of the individual(s) using the email accounts. I know that communications between fraudsters may also

include identifying information about the users of the email or instant message accounts. For example, messages may include names, nicknames, locations, travel plans, or birthdays that can be used to identify the criminal offenders.

22. Based on my training and experience, I know that fraudsters often have several email addresses. Multiple email accounts are used because accounts often get closed by the email providers when they receive information regarding the email account being used in fraud schemes. Email accounts used by the individuals conducting the fraud schemes for non-criminal communication may still contain evidence of the identity of the individual(s) using the SUBJECT EMAIL ACCOUNT.

23. Based on my training and experience, I know that fraudsters often search the Internet when devising and carrying out their schemes. For example, they may research properties to offer for sale, deeds associated with the properties, pricing, methods of payment, and account services to hold their money. They may also bookmark webpages they consider useful so they can return to them easily.

PAST EFFORTS TO OBTAIN THIS EVIDENCE

24. The evidence described in Attachment B has not been previously available to me or other agents.

25. A preservation letter was provided to Google LLC on March 11, 2023.

BACKGROUND REGARDING EMAIL PROVIDER'S SERVICES

26. In my training and experience, I have learned that the EMAIL PROVIDER provides the public with a variety of on-line services, including electronic mail ("email") access, to the public. The EMAIL PROVIDER allows subscribers to obtain email accounts under various domain names, including gmail.com for Google LLC, like the email account listed in Attachment

A. Subscribers obtain an account by registering with the EMAIL PROVIDER. During the registration process, the EMAIL PROVIDER asks subscribers to provide basic personal information, which may include name, address, phone numbers, payment information, and other personal information. Therefore, the computers of the EMAIL PROVIDER are likely to contain stored electronic communications (including retrieved and unretrieved email for the EMAIL PROVIDER's subscribers) and information concerning subscribers and their use of the EMAIL PROVIDER's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

27. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

28. In general, an email that is sent to an EMAIL PROVIDER's subscriber is stored in the subscriber's "mailbox" on the EMAIL PROVIDER's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the EMAIL PROVIDER's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the EMAIL PROVIDER's servers for a certain period of time.

29. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by the EMAIL PROVIDER but may not include all of these categories of data.

30. Subscribers to the EMAIL PROVIDER's services can also store files, including emails, address books, contact or buddy lists, calendar data, photographs, and other files, on servers maintained and/or owned by the EMAIL PROVIDER. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, attachments to emails, including photographs and files, and photographs and files stored in relation to the account.

31. A subscriber to a Google Gmail account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google LLC. For example, Google LLC offers users a calendar service that users may utilize to organize their schedule and share events with others. Google LLC also offers users a service called Google Drive that may be used to store data and documents. The Google Drive service may be used to store documents including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Drive allows users to share their documents with others or the public depending on the settings selected

by the account holder. Google LLC also provides its users with access to photo storage, which can be used to create photo albums, store photographs, and share photographs with others.

32. Additionally, based on my training and experience, as well as Google's Privacy Policy, I know that Google LLC also collects information about users, including information about the devices on which they access their accounts, the devices' hardware models, operating system versions, unique device identifiers, and mobile network information including phone number, location information, and search queries. This information is evidence that can be used to identify and find the individuals conducting the fraud.

33. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. This application seeks a warrant to search all responsive records and information under the control of the EMAIL PROVIDER, which is subject to the jurisdiction of this Court, regardless of where the EMAIL PROVIDER has chosen to store such information.

35. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

36. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

37. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner.

38. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

39. Based on my training and experience, I know that some email providers, including Google LLC, often use internet cookie files to track user information. These “cookies” may allow the email providers to collect information about the account users’ computers, including

information about other accounts accessed by a computer containing the email provider's "cookie." Specifically, the EMAIL PROVIDER may collect information about other email accounts with their service that were accessed by the computers that also accessed the email accounts described in Attachment A. Information regarding other email accounts accessed from the same computer(s) that accessed the email accounts described in Attachment A may provide important evidence about the person using both accounts, including his/her identity and location, as well as the full extent of the fraud.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

40. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit the EMAIL PROVIDER and their agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to the EMAIL PROVIDER with direction that it identify the relevant account(s) described in Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachment B of this affidavit and provide a copy of the specified account and records.

41. I, and/or other law enforcement personnel, will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

42. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified

continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

REQUEST FOR NON-DISCLOSURE

43. I further request that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Google LLC be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for a period of six months. Such an order is justified because notification of the existence of this warrant would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

CONCLUSION


44. Based on the forgoing, there is probable cause to believe the SUBJECT EMAIL ACCOUNT is being used to facilitate the TARGET OFFENSES and that evidence of the crimes will be found within the contents of the SUBJECT EMAIL ACCOUNT. I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§

2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on the EMAIL PROVIDER, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. Accordingly, by this Affidavit and Warrant, I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

/s/ Jason Baumgardner
Special Agent Jason Baumgardner
IRS Criminal Investigation

On this day, the applicant appeared before me by reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.



The Hon. L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina